EXHIBIT B

Excerpts of SW-SEC00001497

solarwinds

SECURITY & COMPLIANCE PROGRAM QUARTERLY OVERVIEW

AUGUST 16, 2019

PROTECT

Highlights

- Access and privilege to critical systems / data is inappropriate. Need to improve internal processes | procedures
- Comprehensive firewall protection for Corporate IT and web properties (Palo Alto Next Gen firewalls in place (58) | Web Application Firewalls (WAF) on all key marketing properties)
- Improved end point protection. End user devices coverage: 80% SEP | 85% encryption | 95% DLP. IT servers coverage: 91% SEP. Hosted environment assessment WIP
- Moving towards Zero Trust model (where we loosely protect all and strongly protect those that can-do material harm). Less requirements on VPN
- Spam / Phishing still a challenge. Adversaries are getting better. Increase in whale phishing (55 million messages blocked 1H2019)
- Movement to make Azure AD authoritative source of identity. Plan to enable federation for all critical assets
- Additional monitoring via SOC is planned for 2nd half of the year

Security Category	Objective	NIST Maturity Level
Next Generation Firewalls	Palo Alto Firewalls are deployed and actively monitored across the company	**5**
Web Application Firewalls	WAFs are deployed for marketing properties but not for production products	**3**
Endpoint Protection and Encryption	Endpoint protection and encryption is deployed and actively managed across the company	**4**
Data Leakage Protection	Data leakage protection is deployed across the company and actively monitored	**3**
Spam / Phishing Detection / Response	Email protections are in place to monitor spam, detect phishing and deter known email scammers	**3**
Authentication, Authorization and Identity Management	User identity, authentication and authorization are in place and actively monitored across the company	**1**
	Protect Maturity Level	**3.2**